Security Quickie 7

This week's Security Quickie: E-mail Etiquette

Unto my good and gentle co-workers of the most wondrous State of Iowa does this missive bring greetings and salutations on this glorious 21st of November…

Hmm… letter writing isn't quite what it used to be. But just like the writing styles of the past, e-mail has its own particular etiquette. Since e-mail has become so prevalent and depended upon for our daily work, it behooves us to know what guidelines we should follow when using this most wonderful method of discourse.

A user should have in mind the following guidelines when writing and opening e-mail:

- Do not send confidential or sensitive information in any form through e-mail. It is each employee's responsibility to determine the confidentiality of each e-mail message they send, using guidelines provided by your agency. Also, assume that any message or information sent using the Internet is available to the public. Never put in a mail message anything you would not put on a postcard, unless the message is encrypted.
- Do not open an e-mail that is of a questionable nature, such as when it has an unusual attachment, it is from an unknown sender, or it is not expected. When opening attachments, macros should be disabled when prompted for. The vast majority of documents and spreadsheets do not require the use of macros, and macro viruses are the most prevalent virus type. If macros are required, ensure the file is from a trusted source and is scanned by anti-virus software. In addition, Outlook's AutoPreview and Preview Pane features should be turned off. These automatically open messages, and can thus automatically open infected messages too, without any assistance from you. Use only the mail client provided by your technical staff. Using another client bypasses at least two levels of virus protection. An accidentally opened mail message containing a virus-infected attachment could wreak havoc not only on a user's computer, but on the department's network as well. *(Truly a fearful prospect…)*
- If you forward or reply to a message you have received, do not change the original wording.
- Never send chain letters via electronic mail. Chain letters are forbidden on the Internet. *By forwarding these thy mail administrator shall be wroth with thee, and justly so. Instead, delete these foul messages and cast them into oblivion.*
- Be conservative in what you send and liberal in what you receive. You should not send heated messages, even if you are provoked.
- Be careful when addressing e-mail. An address might appear to be for an individual but in reality could be for a group. Know to whom you are sending.
- Remember that the recipient is a human being whose culture, language, and humor have different points of reference from your own. Be especially careful with sarcasm.
- Use both upper and lower case characters where appropriate. UPPER CASE LOOKS AS IF YOU ARE SHOUTING.
- Mail and news are subject to forgery and spoofing. Apply common sense before assuming a message is valid. While hoaxes do not actually infect systems like a virus or a Trojan-Horse program, they are still time consuming and thus a drain on departmental resources.

If you have any questions regarding the validity of an e-mail you have received, contact your mail administrator, your agency network security personnel, the ITD Help Desk, or Enterprise Security. If you receive e-mail that appears questionable from someone you know, give him or her a call. Depending on your agency's policy, occasional e-mail of a personal nature may be sent and received as long as it does not disrupt operations, detract from work tasks, or otherwise violate departmental or state policy.